PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-345664
(43)Date of publication of application : 05.12.2003

(51)Int.Cl. G06F 12/14
G06F 1/00
H04L 9/14

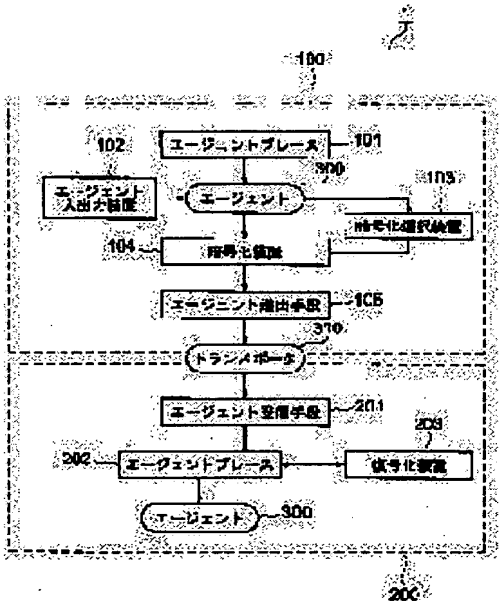
(21)Application number : 2002-156931
(22)Date of filing : 30.05.2002

(71)Applicant : NISSAN MOTOR CO LTD
(72)Inventor : UEDA TETSUO

(54) TRANSMISSION DEVICE, DATA PROCESSING SYSTEM, AND DATA PROCESSING PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To prepare an autonomous program which manages security by itself by performing ciphering with optimum efficiency placing a small load on a computer resource while holding ciphering strength.
SOLUTION: In a transmission-side system 100, an agent place 101 generates an agent 300 having a program and data and sets a term of validity thereto. Further, a ciphering selecting device 103 selects a ciphering method which is strong enough not to allow illegal deciphering within the term of validity and a ciphering device 104 ciphers the agent. The this is sent from an agent sending- out means 105 to a reception-side system 200. After the term of validity expires, the agent disappears by itself. Therefore, data are ciphered within the term of validity, so illegal deciphering is no allowed and after the term of validity expires, the data are deleted, so that access is disabled even when deciphering is performed. The security of the data is properly ensured by the proper ciphering in which processing efficiency is taken into consideration.

図1



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－345664
（P2003－345664A）
(43)公開日　平成15年12月５日(2003.12.5)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ	テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ　５Ｂ０１７
			３２０Ｂ　５Ｂ０７６
			３２０Ｄ　５Ｊ１０４
1/00		9/06	６６０Ｌ
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１

審査請求　未請求　請求項の数19　ＯＬ　（全 13 頁）

(21)出願番号　特願2002－156931(P2002－156931)

(22)出願日　平成14年５月30日(2002.5.30)

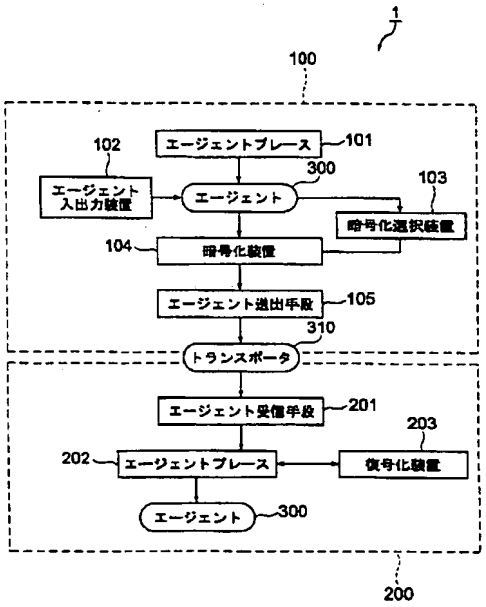
(71)出願人　000003997
日産自動車株式会社
神奈川県横浜市神奈川区宝町２番地
(72)発明者　上田　哲郎
神奈川県横浜市神奈川区宝町２番地　日産自動車株式会社内
(74)代理人　100099900
弁理士　西出　眞吾　（外２名）

Ｆターム(参考)　5B017 AA06 AA07 BA08 BB09 BB10
CA15 CA16
5B076 FA01 FB18
5J104 AA12 AA16 AA36

(54)【発明の名称】　送信装置、データ処理システム及びデータ処理プログラム

(57)【要約】
【課題】暗号化強度を保ちつつ計算機リソースへの負荷が少ない効率が最適な暗号化を行い自らセキュリティを管理する自律型プログラムを生成する。
【解決手段】送信側システム１００においては、エージェントプレース１０１がプログラム及びデータを有するエージェント３００を生成し、これに有効期限を設定する。また、暗号化選択装置１０３で有効期限内に不正に復号化されない程度の強度の暗号化方法を選択し、暗号化装置１０４でエージェントを暗号する。そして、これをエージェント送出手段１０５より受信側システム２００に送信する。なお有効期限が満了したらエージェントは自ら消滅する。従って、有効期限内はデータは暗号化されているので不正な復号化は許されず、有効期限満了後はデータが消滅しているので復号化されてもアクセスできない。従って、処理効率も考慮した適度な暗号化によりデータのセキュリティ性が適切に確保される。

図 1



1

【特許請求の範囲】

【請求項１】計算機装置間を移動して実行されるプログラム及び任意のデータを有するオブジェクトを生成するオブジェクト生成手段と、

前記生成されたオブジェクトに対して、有効期限を設定する有効期限設定手段と、

前記設定された有効期限内に不正な方法により復号化されることが無い適切な強度の暗号化方法を選択する暗号化方法選択手段と、

前記選択された暗号化方法により前記オブジェクトの前記データを暗号化する暗号化手段と、

前記データの暗号化されたオブジェクトを他の前記計算機装置に送信する送信手段とを有する送信装置。

【請求項２】前記オブジェクトは、前記有効期限が満了した場合に自律的に消滅する請求項１に記載の送信装置。

【請求項３】前記オブジェクトが有する前記プログラムは、前記有効期限が満了した場合に当該オブジェクトを自律的に消滅させるための記述を含む請求項２に記載の送信装置。

【請求項４】前記オブジェクトが有する前記プログラムは、所望の処理を実行するための記述及び前記所望の処理の終了後に当該オブジェクトを自律的に操作するための記述を含む請求項１～３のいずれかに記載の送信装置。

【請求項５】前記オブジェクトを自律的に操作するための記述は、他の計算機装置に移動するためのオブジェクトを複製するための記述、当該オブジェクトを消滅するための記述、及び、送信元の計算機装置へ帰着するための記述の、少なくともいずれか１つを含む請求項４に記載の送信装置。

【請求項６】前記暗号化方法選択手段は、復号鍵を知らずに復号化しようとした場合に復号化に要する時間が前記設定した有効期限よりも長く、かつできるだけ暗号化処理が容易な暗号化方法を選択する請求項１～５のいずれかに記載の送信装置。

【請求項７】前記暗号化方法選択手段は、暗号化アルゴリズムを選択し、

前記暗号化手段は、前記選択された暗号化アルゴリズムにより、前記データを暗号化する請求項１～６のいずれかに記載の送信装置。

【請求項８】前記暗号化方法選択手段は、鍵の長さを選択し、

前記暗号化手段は、前記選択された長さの鍵を用いて前記データを暗号化する請求項１～７のいずれかに記載の送信装置。

【請求項９】複数の計算機装置がネットワークを介して接続されたデータ処理システムであって、

計算機装置上で実行されるプログラム及び任意のデータを有するオブジェクトを生成するオブジェクト生成手段

2

と、

前記生成されたオブジェクトに対して、有効期限を設定する有効期限設定手段と、

前記設定された有効期限内に、不正な方法により復号化されることが無い適切な強度の暗号化方法を選択する暗号化方法選択手段と、

前記選択された暗号化方法により前記オブジェクトの前記データを暗号化する暗号化手段と、

前記データの暗号化されたオブジェクトを送信する送信手段とを有する第１のデータ処理装置と、

前記送信されたオブジェクトを受信する受信手段と、

前記受信したオブジェクトに設定されている前記有効期限内である場合に、前記暗号化されたデータを復号化し、前記オブジェクトが有するプログラムを実行するプログラム実行手段と、

前記受信したオブジェクトに設定されている前記有効期限が満了した場合に、前記オブジェクトを消滅させるオブジェクト消滅手段とを有する第２のデータ処理装置とを有するデータ処理システム。

【請求項１０】前記暗号化方法選択手段は、復号鍵を知らずに復号化しようとした場合に復号化に要する時間が前記設定した有効期限よりも長く、できるだけ暗号化処理が容易な暗号化方法を選択する請求項９に記載のデータ処理システム。

【請求項１１】前記暗号化方法選択手段は、暗号化アルゴリズムを選択し、

前記暗号化手段は、前記選択された暗号化アルゴリズムにより、前記送信対象のデータを暗号化する請求項９又は１０に記載のデータ処理システム。

【請求項１２】前記暗号化方法選択手段は、鍵の長さを選択し、

前記暗号化手段は、前記選択された長さの鍵を用いて前記送信対象のデータを暗号化する請求項９～１１のいずれかに記載のデータ処理システム。

【請求項１３】前記オブジェクトが有する前記プログラムは、所望の処理を実行するための記述及び当該オブジェクトを自律的に操作するための記述を含み、

前記オブジェクト消滅手段においては、前記オブジェクトの前記プログラムが実行されることにより、当該オブジェクトの有効期限が満了した場合に該オブジェクトが消滅される請求項９～１２のいずれかに記載のデータ処理システム。

【請求項１４】前記オブジェクトが有する前記プログラムは、所望の処理を実行するための記述、及び、前記所望の処理の終了後に当該オブジェクトを自律的に操作するための記述を含み、

前記プログラム実行手段においては、前記オブジェクトの前記プログラムが実行されることにより、前記所望の処理が終了した後において前記オブジェクトが自律的に操作される請求項９～１３のいずれかに記載のデータ処

理システム。
【請求項１５】前記所望の処理の終了後に当該オブジェクトを自律的に操作するための記述は、さらに他の計算機装置に移動するために当該オブジェクトを複製するための記述、当該オブジェクトを消滅するための記述、及び、送信元の計算機装置へ帰着するための記述の少なくともいずれか１つを含む請求項１４に記載のデータ処理システム。
【請求項１６】コンピュータ上において所望の処理を実行するプログラム及び任意のデータを有するオブジェクトであるデータ処理プログラムであって、
前記コンピュータ上で前記データを参照して所望の処理を行う第１の機能と、予め設定された有効期限が満了したか否かを検出する第２の機能と、
前記有効期限が満了した場合に、当該オブジェクトを消滅させる第３の機能とをコンピュータに実現させるデータ処理プログラム。
【請求項１７】前記設定された前記オブジェクトの有効期限内に不正な方法により復号化されることが無い適切な強度の暗号化方法により、前記データが暗号化されている請求項１６に記載のデータ処理プログラム。
【請求項１８】前記第１の機能による前記所望の処理の終了後に、前記オブジェクトを自律的に操作する第４の機能をさらにコンピュータに実現させる請求項１６又は１７に記載のデータ処理プログラム。
【請求項１９】前記第４の機能は、他の計算機装置にさらに移動するために前記オブジェクトを複製する、前記オブジェクトを消滅する、及び、当該オブジェクトの生成元に帰着するの、少なくともいずれか１つの機能を実現する請求項１８に記載のデータ処理プログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、モバイルエージェントと言われる自律型のプログラムオブジェクトを用いて複数の計算機装置が接続されたネットワーク上において所望の処理を行うデータ処理システム、そのモバイルエージェントを生成してネットワーク上に送出する送信装置、及び、そのモバイルエージェントに含まれて実際にコンピュータ上においてそれらの処理を実現するデータ処理プログラムに関する。
【０００２】
【従来の技術】一般的に、ソフトウエアプログラムは、スタンドアローン型及びクライアントサーバ型に大別される。スタンドアローン型は、計算機固有に記述されたネイティブなプログラムを直接ターゲットマシンにインストールして用いる方法である。一方、クライアントサーバ型は、クライアントマシン（ターゲットマシン）に搭載されたクライアントソフトウエアと、サーバに搭載されたサーバソフトウエアが協調して処理を行う方法であり、インターネットが普及した現在では、主にウェブベースアプリケーションのことを指している場合が多い。ウェブベースアプリケーションは、実際にユーザが用いるプログラムはサーバ側にあり、ユーザはターゲットマシンに汎用的なＷＷＷブラウザをインストールし、これよりネットワークを介してサーバ側プログラムを用いる方法である。
【０００３】スタンドアローン型のメリットは、一般にプログラムがターゲットマシン固有に記述されているため処理が高速であるという点が挙げられる。また、ネットワークの利用が最低限で済むため、スピードの遅いネットワーク環境等においても、クライアントサーバ型のようにこのネットワークの遅さがボトルネックにならず、高速な処理が可能であるという点も挙げられる。
【０００４】一方、スタンドアローン型のデメリットは、ユーザが、利用する全てのターゲットマシンに１つ１つソフトウエアプログラムをインストールしなければならないという点が挙げられる。ソフトウエアは、バージョンアップが宿命と言えるが、その度に、バージョンアップの手続き及びインストール処理を行わなければならず、大きな問題と言える。また、スタンドアローンシステムにおいては、一般に、ソフトウエアベンダー側がパッケージ化して用意したソフトウエア群をインストールして利用する場合が多いが、ユーザは必ずしもその全ての機能を必要としているわけではない場合がある。しかしながら、そのような場合も、ユーザは不必要な機能をも含む全てのソフトウエアプログラムをインストールせざるを得ず、必要な機能だけを必要な時にだけ利用するといった利用形態を実現することが難しい。その結果、計算機のリソースを圧迫することとなり、特に、モバイル端末のような記憶容量が限られており計算機リソースの浪費を抑えたいという環境下では問題である。
【０００５】また、クライアントサーバ型のメリットは、ユーザはＷＷＷブラウザさえ用意すればよく特別なソフトウエアのインストールの必要が無いという点が挙げられる。クライアントサーバ型は、ＷＷＷブラウザを用いて、必要な時に必要な機能のみをネットワークを介してサーバ装置より呼び出し利用するという形態であるため、利用するアプリケーションのバージョンは常に最新のものであるし、利用しない時にはソフトウエアプログラムは計算機中に存在せず、計算機リソースを浪費することが無い。なお、このようなクライアントサーバ型のメリットから、ＡＳＰ（Application Service Provider）と呼ばれるアプリケーションプログラムの時間貸し業が注目されている。
【０００６】クライアントサーバ型のデメリットは、ネットワークのボトルネックである。クライアントサーバ型では、表示や操作がクライアント側にあり、実際の処理はサーバ側で行うため、クライアントとサーバの間で頻繁にデータのやり取りが必要となり、データの授受を受け持つネットワークの性能がボトルネックとなる。例

えば、スタンドアローン型のシステムでは一瞬でできる処理も、クライアントサーバ型ではネットワークの遅延の影響を受け、待機時間が必要となる。一般に、ネットワークのスピードはメモリアクセス等のバススピードやＣＰＵの処理スピードよりも遥かに遅いので、ネットワークの転送スピードがボトルネックになるのである。また、クライアントサーバ型のデメリットとして、一般にWWWブラウザのグラフィカルな表現力、インタフェースが限られたものであり、スタンドアローン型の多彩な表現やインタフェースに及ばないという問題もある。

【０００７】ところで、このようなクライアントサーバ型とスタンドアローン型の中間的なアプローチで両方のメリットを享受しようとする試みに、Ｊａｖａアプレットのようなプログラム逐次ダウンロード型のアプリケーションがある。近年広く使用されているいわゆるｉモード携帯電話のｉアプリケーションも、この種のアプリケーションの１つである。これは、ユーザはクライアントサーバ型の場合と同じくWWWブラウザのみをマシン内に備えるが、サーバ側にあるプログラムをその状態で使用するのではなく、WWWブラウザに一時的にダウンロードして用いるものである。これによって、従来のクライアントサーバ型では、ユーザの操作に応じて頻繁にクライアントとサーバとの間でデータ交換が必要であったものが、プログラムがクライアント側に移動していることにより、データ交換が不要となり、クライアントサーバ型で問題となっていたネットワークボトルネックの問題を解消できるのである。

【０００８】このタイプのプログラムは、最初のダウンロードにのみ時間がかかるが、その後は保存しておくこともできるので、まさにスタンドアローン型とクライアントサーバ型のメリットのみを持っていると言える。また、グラフィカルユーザインタフェースにおいても、Ｊａｖａアプレットの場合では、同じWWWブラウザを用いながらスタンドアローン型とほぼ同程度な高度なインタフェースを実現できている。実際には、Ｊａｖａアプレットにはセキュリティや互換性（インターオペラビリティ）に問題があるが、分散型のアプリケーションの向かうべき方向性を示していると言える。

【０００９】このようなソフトウエアプログラムの実現形態の延長上にあるものとして、いわゆるモバイルエージェント型プログラムが挙げられる。このモバイルエージェント型プログラムについて、Ｊａｖａアプレットのようなダウンロード型のプログラムと比較して説明する。ダウンロード型プログラムは、ユーザの要請によってサーバ側からダウンロードされ、ユーザが利用している間、ダウンロードされた計算機中に滞在して処理を行い、ユーザの利用が終わると終了して消滅するプログラムである。これに対して、モバイルエージェント型プログラムは、同じく計算機から計算機にプログラム本体がダウンロードされ、利用されるが、モバイルエージェント自体が自律的に計算機の間を形を変えて移動したり、自身のクローンを作ったりして、それらの協調によりユーザの要求を処理するものである。端的な例で言えば、ダウンロード型プログラムがユーザの指示でダウンロードされるのに対して、モバイルエージェント型プログラムは、ユーザの指示によってユーザの要求をもってネットワークに出て行き、複数の計算機上でユーザの指示を実行して、戻ってくる（応えを持ち帰る）プログラムである。

【００１０】

【発明が解決しようとする課題】ところで、このようなモバイルエージェント型プログラムは、ユーザの個人データのような機密データを持ち歩くケースも少なくない。例えば、モバイルエージェントが、個人の情報を持って航空機やホテルの予約のためにインターネットに出て行く場合等である。このような場合、従来のダウンロード型プログラムでは、サーバとクライアントの間のセキュアな通信さえ確保されていればデータのセキュリティ性が確保できていた。しかしながら、モバイルエージェント型プログラムでは、ユーザが送り出した後のエージェントの動作はもはやユーザからは制御できないため、管理できる範囲の通信のセキュリティを確保した程度では全体としてのセキュリティ性が確保されたとは言えないという事態となる。従って、モバイルエージェント型プログラムを用いたシステムにおいては、モバイルエージェント自らがデータ等のセキュリティ性を管理できるようにしたいという要望がある。

【００１１】一方、データのセキュリティ性を確保するためには、データを暗号化することが考えられる。データの暗号化は、データの送り手と受け手が暗号鍵を共有化することによってデータを暗号化しデータの授受を排他的に行う仕組みであり、ＤＥＳ（Data Encryption Standard）のような共有鍵方式や、ＲＳＡ（ronald Rivest, adi Shamir, lenard Adleman）等の秘密鍵方式が知られている。一般に、鍵の長さを例にとった場合、鍵長が長いほど暗号の強度が高まり安全であると言える。しかし、鍵長が長いほど、暗号化／復号化にも時間を要し、計算機リソースに相当の負荷を与えることとなる。この暗号化強度と計算機リソースの負荷の問題は、暗号化アルゴリズムの種類についても同様である。

【００１２】モバイルエージェント型プログラムの場合には、汎用性や応答性等を維持するために、計算機リソースやネットワークリソースを無駄に浪費しないように考慮する必要がある。従って、このような暗号化を適用する場合においても、セキュリティ性を確保できるよう暗号化の強度を保ちつつ、計算機リソースへの負荷がなるべく抑えられるような、すなわち効率が最適となるような暗号化を行いたいという要望がある。そして、そのために、モバイルエージェントが保護しようとしているデータに最適な暗号強度を選択したいという要望があ

る。

【００１３】なお、保護すべきデータに応じて鍵やアルゴリズムを動的に変化させる方法としては、例えば特開平９－２５８９９号公報に開示されている計算機中のＣＰＵが処理するメモリ内部に蓄積されたデータを保護する手法がある。この手法によると、メモリ内のデータの暗号化／復号化を単調にいつも同じアルゴリズムや鍵を使っていたのでは、そのうちアルゴリズムや鍵が明らかになって暗号化の意味がなくなる心配があるので、データそのものの属性、つまり、メモリ上のアドレスや仮想記憶ページ番号等をキーにハッシュすることによって、暗号化／復号化の鍵やアルゴリズムを動的に変化させるというものである。しかしながらこの手法は、ランダムに鍵やアルゴリズムを選択することによって、暗号化／復号化の強度を高めようとするものであり、暗号化対象のデータに最適の鍵やアルゴリズムを動的に選択し、暗号化の強度を保ったままで最大の効率を確保するという目的を達成するものではない。

【００１４】また、特開平１１－２８２７５３号公報や、特開平１０－３４０２５５号公報には、暗号そのものに有効期限を定めて期限を越えて復号化されないようにすることによって、セキュリティを高める方法が開示されている。しかし、この方法は、有効期限を設けることにより暗号化システムへの長期に渡る不正な復号処理の試行に歯止めをかけることを目的とするものであり、暗号化方法自体のセキュリティ性、計算機負荷の妥当性等について関わるものではなく、そのことについては何ら記載も示唆もされていない。

【００１５】本発明はこのような問題点に鑑みてなされたものであって、本発明の目的は、暗号化の強度を保ちつつ計算機リソースへの負荷が抑えられるような効率が最適な暗号化方法を用いてセキュリティ性を自ら管理することができるモバイルエージェントを送信する送信装置を提供することにある。また、本発明の他の目的は、暗号化の強度を保ちつつ計算機リソースへの負荷が抑えられるような効率が最適な暗号化方法を用いてセキュリティ性を自ら管理することができるモバイルエージェントを用いて、ネットワーク上において効率よくセキュリティ性の確保された所望のデータ処理を行うことができるデータ処理システムを提供することにある。さらに、本発明の他の目的は、暗号化の強度を保ちつつ計算機リソースへの負荷が抑えられるような効率が最適な暗号化方法を用いてセキュリティ性を自ら管理することができ、その状態でネットワーク環境上において所望の処理を実行するモバイルエージェントたるデータ処理プログラムを提供することにある。

【００１６】

【課題を解決するための手段】前記目的を達成するために、本発明の第１の観点によれば、本発明の送信装置は、計算機装置間を移動して実行されるプログラム及び任意のデータを有するオブジェクトを生成するオブジェクト生成手段と、前記生成されたオブジェクトに対して、有効期限を設定する有効期限設定手段と、前記設定された有効期限内に、不正な方法により復号化されることが無い適切な強度の暗号化方法を選択する暗号化方法選択手段と、前記選択された暗号化方法により前記オブジェクトの前記データを暗号化する暗号化手段と、前記データの暗号化されたオブジェクトを他の前記計算機装置に送信する送信手段とを有する（請求項１）。

【００１７】このような構成の送信装置によれば、オブジェクト生成手段において計算機装置間を移動して実行されるプログラム及び任意のデータを有するオブジェクトを生成し、その生成されたオブジェクトに対して、有効期限設定手段において有効期限を設定する。そして、暗号化方法選択手段により、その設定された有効期限内に、不正な方法により復号化されることが無いような適切な強度の暗号化方法を選択し、暗号化手段においてその選択された暗号化方法により前記オブジェクトの前記データを暗号化している。そして、これら暗号化データを有し有効期限を設定されたオブジェクトを、所望の他の前記計算機装置に送信する。従って、オブジェクトが有効な期間はデータは暗号化されており不正な復号化を許さないので、データのセキュリティが確実に確保される。また一方で、その有効期限後はデータが消滅されるので、暗号化によりセキュリティを確保する必要が無い。すなわち、有効期限満了後は、データ自身が消滅されているので、極端に言えば暗号化が不正に解読されることとなっても差し障りが無い。従って、暗号化方法選択手段における暗号化方法選択の際には、有効期限内のみ有効であるような適度の暗号化強度の暗号化方法を選択すればよく、結果的に過剰な暗号化強度を有し処理が複雑な暗号化方法を選択する必要がなくなる。

【００１８】好適には、前記オブジェクトは、前記有効期限が満了した場合に自律的に消滅する（請求項２）。また好適には、前記オブジェクトが有する前記プログラムは、前記有効期限が満了した場合に当該オブジェクトを自律的に消滅させるための記述を含む（請求項３）。また好適には、前記オブジェクトが有する前記プログラムは、所望の処理を実行するための記述及び前記所望の処理の終了後に当該オブジェクトを自律的に操作するための記述を含む（請求項４）。具体的かつ好適な例としては、前記オブジェクトを自律的に操作するための記述は、他の計算機装置にさらに移動するために当該オブジェクトを複製するための記述、当該オブジェクトを消滅するための記述、及び、送信元の計算機装置へ帰着するための記述の、少なくともいずれか１つを含む（請求項５）。

【００１９】また好適には、前記暗号化方法選択手段は、復号鍵を知らずに復号化しようとした場合に復号化に要する時間が前記設定した有効期限よりも長く、かつ

できるだけ暗号化処理が容易な暗号化方法を選択する（請求項６）。また好適には、前記暗号化方法選択手段は、暗号化アルゴリズムを選択し、前記暗号化手段は、前記選択された暗号化アルゴリズムにより、前記データを暗号化する（請求項７）。また好適には、前記暗号化方法選択手段は、鍵の長さを選択し、前記暗号化手段は、前記選択された長さの鍵を用いて前記データを暗号化する（請求項８）。

【００２０】また、本発明の第２の観点によれば、本発明のデータ処理システムは、複数の計算機装置がネットワークを介して接続されたデータ処理システムであって、計算機装置上で実行されるプログラム及び任意のデータを有するオブジェクトを生成するオブジェクト生成手段と、前記生成されたオブジェクトに対して、有効期限を設定する有効期限設定手段と、前記設定された有効期限内に、不正な方法により復号化されることが無い適切な強度の暗号化方法を選択する暗号化方法選択手段と、前記選択された暗号化方法により前記オブジェクトの前記データを暗号化する暗号化手段と、前記データの暗号化されたオブジェクトを送信する送信手段とを有する第１のデータ処理装置と、前記送信されたオブジェクトを受信する受信手段と、前記受信したオブジェクトに設定されている前記有効期限内である場合に、前記暗号化されたデータを復号化し、前記オブジェクトが有するプログラムを実行するプログラム実行手段と、前記受信したオブジェクトに設定されている前記有効期限が満了した場合に、前記オブジェクトを消滅させるオブジェクト消滅手段とを有する第２のデータ処理装置とを有する（請求項９）。

【００２１】このような構成のデータ処理システムにおいては、第１のデータ処理装置のオブジェクト生成手段においてプログラム及び任意のデータを有するオブジェクトを生成し、その生成されたオブジェクトに対して有効期限設定手段において有効期限を設定する。また、その設定された有効期限内に、不正な方法により復号化されることが無い適切な強度の暗号化方法を暗号化方法選択手段において選択し、暗号化手段においてその選択された暗号化方法により前記オブジェクトのデータを暗号化する。そして、このプログラム及び暗号化データを有するオブジェクトが送信手段よりネットワークを解して所望の第２のデータ処理装置に送信される。第２のデータ処理装置においては、この送信されたオブジェクトを受信手段において受信し、設定されている有効期限の期間内である場合に、プログラム実行手段により暗号化されたデータを復号化してプログラムを実行する。また、有効期限が満了した場合には、オブジェクト消滅手段が記オブジェクトを消滅させる。従って、オブジェクトが有効な期間はデータは暗号化されており不正な復号化を許さないので、データのセキュリティが確実に確保される。また一方で、その有効期限後はデータが消滅されるので、暗号化によりセキュリティを確保する必要が無い。すなわち、有効期限満了後は、極端に言えば暗号化が不正に解読されることとなっても差し障りが無い。データ自身が消滅されているからである。従って、暗号化方法選択手段における暗号化方法選択の際には、有効期限内のみ有効であるような適度の暗号化強度の暗号化方法を選択すればよく、結果的に過剰な暗号化強度を有し処理が複雑な暗号化方法を選択する必要がなくなる。

【００２２】好適には、前記暗号化方法選択手段は、復号鍵を知らずに復号化しようとした場合に復号化に要する時間が前記設定した有効期限よりも長く、できるだけ暗号化処理が容易な暗号化方法を選択する（請求項１０）。また好適には、前記暗号化方法選択手段は、暗号化アルゴリズムを選択し、前記暗号化手段は、前記選択された暗号化アルゴリズムにより、前記送信対象のデータを暗号化する（請求項１１）。また好適には、前記暗号化方法選択手段は、鍵の長さを選択し、前記暗号化手段は、前記選択された長さの鍵を用いて前記送信対象のデータを暗号化する（請求項１２）。また好適には、前記オブジェクトが有する前記プログラムは、所望の処理を実行するための記述及び当該オブジェクトを自律的に操作するための記述を含み、前記オブジェクト消滅手段においては、前記オブジェクトの前記プログラムが実行されることにより、当該オブジェクトの有効期限が満了した場合に該オブジェクトが消滅される（請求項１３）。

【００２３】また好適には、前記オブジェクトが有する前記プログラムは、所望の処理を実行するための記述、及び、前記所望の処理の終了後に当該オブジェクトを自律的に操作するための記述を含み、前記プログラム実行手段においては、前記オブジェクトの前記プログラムが実行されることにより、前記所望の処理が終了した後において前記オブジェクトが自律的に操作される（請求項１４）。具体的かつ好適な例としては、前記所望の処理の終了後に当該オブジェクトを自律的に操作するための記述は、さらに他の計算機装置に移動するために当該オブジェクトを複製するための記述、当該オブジェクトを消滅するための記述、及び、送信元の計算機装置へ帰着するための記述の少なくともいずれか１つを含む（請求項１５）。

【００２４】また、本発明の第３の観点によれば、本発明にかかるデータ処理プログラムは、コンピュータ上において所望の処理を実行するプログラム及び任意のデータを有するオブジェクトであるデータ処理プログラムであって、前記コンピュータ上で前記データを参照して所望の処理を行う第１の機能と、予め設定された有効期限が満了したか否かを検出する第２の機能と、前記有効期限が満了した場合に、当該オブジェクトを消滅させる第３の機能とをコンピュータに実現させるデータ処理プログラムである（請求項１６）。

【００２５】このような構成のデータ処理プログラムは、コンピュータに読み込まれてこれにより動作されることにより、第１の機能により具備する記データを参照して所望の処理が行われる。一方で、第２の機能により、予め設定された有効期限が満了したか否かが検出され、有効期限が満了していた場合には、第３の機能によりオブジェクト自らが消滅される。従って、読み込まれたコンピュータや、その背景のネットワーク等の環境に左右されること無く、有効期限がくればこのデータ処理プログラムたるオブジェクト自身が消滅し、保持されるデータ自身も消滅することとなり、これにより１つのセキュリティ性が確保される。また、このような条件があるので、このオブジェクトに含まれるデータを例えば暗号化する際には、この満了期間のみ不正なアクセスに耐え得る暗号化強度の暗号化を行えば十分であり、結果的に過剰な暗号化強度を有し、それがために処理する計算機リソース等に過大な負荷を与えるような暗号化を行うことがなくなる。すなわち、読み込まれて実行される処理環境に対して、不必要な過大な負荷を与えることが無く、処理効率のよいプログラムとなる。

【００２６】好適には、前記設定された前記オブジェクトの有効期限内に不正な方法により復号化されることが無い適切な強度の暗号化方法により、前記データが暗号化されている（請求項１７）。また好適には、前記第１の機能による前記所望の処理の終了後に、前記オブジェクトを自律的に操作する第４の機能をさらに有する（請求項１８）。具体的かつ好適な例としては、前記第４の機能は、他の計算機装置にさらに移動するために前記オブジェクトを複製する、前記オブジェクトを消滅する、及び、当該オブジェクトの生成元に帰着するの、少なくともいずれか１つの機能を実現する（請求項１９）。

【００２７】

【発明の効果】このような構成の請求項１～８に記載の発明によれば、オブジェクト自身に有効期限を設定し、その有効期限までの期間、不正なアクセスからデータを保護することができる暗号化方法で暗号化を行うようにしており、暗号化の強度を保ちつつ計算機リソースへの負荷を必要最小限に抑えることができる。従って、最適な暗号化方法を選択し、セキュリティ性を自らが管理することができるモバイルエージェントを送信する送信装置を提供することができる。これに加えて請求項２に記載の発明によれば、モバイルエージェントは有効期限、すなわち寿命を迎えると送信者から制御されなくとも自動的に消滅し、保持しているデータも失われるので、一定時間（寿命）経過後に不正アクセス、盗聴等が行われることがなくなり、セキュリティが確実に確保される。

【００２８】また、請求項３に記載の発明によれば、オブジェクトの有効期限満了に伴う消滅は、オブジェクト自らが保持するプログラムの記述に基づいて行われるため、ネットワーク上の種々のプログラム実行環境において実行されるオブジェクトにおいては、環境の影響を受けることなく確実にオブジェクトを消滅できることとなり、セキュリティが確実に確保される。また、請求項４に記載の発明によれば、所望の処理の処理結果を含むオブジェクト自身等の処遇を、オブジェクト自らが規定することができ、ネットワーク環境に依存せずオブジェクト自らが管理したセキュリティ確保が可能となる。そして請求項５に記載の発明によれば、所望の処理が終了した後に、他の計算機装置へのさらなるオブジェクトの移動、オブジェクトの消滅、オブジェクト生成元への帰着等のオブジェクトの操作を行うことができる。

【００２９】また、請求項６に記載の発明によれば、少なくともオブジェクトの有効期限の間のみ不正な復号化が不可能であるような暗号化強度で暗号化を行えばよく、過剰な暗号化強度で暗号化を行い計算機リソースを浪費する等の事態を防ぐことができる。また、請求項７に記載の発明によれば、暗号化アルゴリズムを選択することにより、所望の暗号化強度の暗号化方法を選択し暗号化することができる。また、請求項８に記載の発明によれば、鍵長を選択することにより、所望の暗号化強度の暗号化方法を選択し暗号化することができる。

【００３０】また、前述した請求項９～１５に記載の発明によれば、暗号化の強度を保ちつつ計算機リソースへの負荷が抑えられるような効率が最適な暗号化方法を用いてセキュリティ性を自ら管理することができるモバイルエージェントを用いて、ネットワーク上において効率よくセキュリティ性の確保された所望のデータ処理を行うことができるデータ処理システムを提供することができる。これに加えて請求項１０に記載の発明によれば、少なくともオブジェクトの有効期限の間のみ不正な復号化が不可能であるような暗号化強度でなるべく処理が簡単な暗号化方法で暗号化を行えばよく、過剰な暗号化強度で暗号化を行い計算機リソースを浪費する等の事態を防ぐことができる。また、請求項１１に記載の発明によれば、暗号化アルゴリズムを選択することにより、所望の暗号化強度の暗号化方法を選択し暗号化することができる。また、請求項１２に記載の発明によれば、鍵長を選択することにより、所望の暗号化強度の暗号化方法を選択し暗号化することができる。

【００３１】また、請求項１３に記載の発明によれば、オブジェクトの有効期限満了に伴う消滅は、オブジェクト自らが保持するプログラムの記述に基づいて行われるため、ネットワーク上の種々のプログラム実行環境において実行されるオブジェクトにおいては、環境の影響を受けることなく確実にオブジェクトを消滅できることとなり、セキュリティが確実に確保される。また、請求項１４に記載の発明によれば、所望の処理の処理結果を含むオブジェクト自身等の処遇を、オブジェクト自らが規定することができ、ネットワーク環境に依存せずオブジェクト自らが管理したセキュリティ確保が可能となる。

そして請求項１５に記載の発明によれば、所望の処理が終了した後に、他の計算機装置へのさらなるオブジェクトの移動、オブジェクトの消滅、オブジェクト生成元への帰着等のオブジェクトの操作を行うことができる。

【００３２】また、前述した請求項１６～１９に記載の発明によれば、セキュリティ性を自ら管理することができ、その状態でネットワーク環境上において所望の処理を実行するモバイルエージェントたるデータ処理プログラムを提供することができる。これに加えて請求項１７に記載の発明によれば、少なくともオブジェクトの有効期限の間のみ不正な復号化が不可能であるような暗号化強度によりデータが暗号化されているので、過剰な暗号化強度で暗号化を行い計算機リソースを浪費する等の事態を防ぐことができる、効率よい処理を行うデータ処理プログラムを提供することができる。また、請求項１８に記載の発明によれば、所望の処理の処理結果を含むオブジェクト自身等の処遇を、オブジェクト自らが規定することができ、ネットワーク環境に依存せずオブジェクト自らが管理したセキュリティ確保が可能となる。そして請求項１９に記載の発明によれば、所望の処理が終了した後に、他の計算機装置へのさらなるオブジェクトの移動、オブジェクトの消滅、オブジェクト生成元への帰着等の自らの操作を行うことができる。

【００３３】

【発明の実施の形態】本発明の一実施の形態について図１～図４を参照して説明する。本実施の形態においては、モバイルエージェントと言われるオブジェクトをネットワーク上に配置することにより、ネットワーク上で所望のデータ処理を行うデータ処理システムを例示し、特にそのモバイルエージェントの取り扱い方法を説明することにより本発明を説明する。

【００３４】まず、そのデータ処理システムの構成について説明する。図１は、本実施の形態のデータ処理システム１の構成を示すブロック図である。図１に示すように、データ処理システム１は送信側システム１００及び受信側システム２００を有する。また、図示しないが、送信側システム１００と受信側システム２００とは、任意にデータ伝送可能にネットワークにより接続されている。このネットワークは、Ｊａｖａ及びＴＣＰ／ＩＰをベースとしたネットワークであり、本実施の形態においてはインターネットとする。

【００３５】送信側システム１００は、モバイルエージェントを生成しネットワークを介して受信側システム２００に送信する例えばパーソナルコンピュータ等の計算機装置である。送信側システム１００は、エージェントブレース１０１、エージェント入出力装置１０２、暗号化選択装置１０３、暗号化装置１０４及びエージェント送出手段１０５を有する。

【００３６】エージェントブレース１０１は、モバイルエージェント３００のオブジェクトを生成する。具体的

には、送信側システム１００の計算機リソースのメモリ上に、モバイルエージェント３００のオブジェクトを確保することにより、モバイルエージェント３００の実体を生成し、さらにモバイルエージェント３００とエージェントブレース１０１との間で相互に参照可能にポインタを張ることにより、モバイルエージェント３００を登録する。そして、モバイルエージェント３００に独自のスレッドを割り当てることにより、モバイルエージェント３００を起動する。この時、エージェントブレース１０１は、モバイルエージェント３００に、消滅するまでの有効期限（寿命）をセットする。なお、この寿命は、モバイルエージェントごとに個別の値がセットされる。

【００３７】エージェント入出力装置１０２は、モバイルエージェント３００に対する指示等を入力する。モバイルエージェント３００に特段の指示等がある場合には、エージェントブレース１０１におけるモバイルエージェント３００の生成後に送信側システム１００は入力フェーズに入る。その結果、エージェント入出力装置１０２に適宜必要なダイアログボックス等が表示されて、所望の指示が入力される。

【００３８】暗号化選択装置１０３は、モバイルエージェント３００が保持しているデータを暗号化するための暗号化条件を選択する。暗号化選択装置１０３は、モバイルエージェント３００に設定されているモバイルエージェント３００の寿命、及び、モバイルエージェント３００のサイズに基づいて、暗号化強度が最適となるような暗号化条件を選択し、その条件でモバイルエージェント３００が保持するデータの暗号化を行うよう、実質的に暗号化装置１０４に指示する。より具体的には、具備している暗号化アルゴリズムより最適な暗号化アルゴリズムを選択し、また、その暗号化アルゴリズムに対して最適な鍵長を検索し、その暗号化アルゴリズム及び鍵長を暗号化装置１０４に指定する。なお、暗号化選択装置１０３における暗号化条件の選択基準等については、後に詳細に説明する。

【００３９】暗号化装置１０４は、暗号化選択装置１０３より指定された暗号化アルゴリズム及び鍵長により、モバイルエージェント３００が保持するデータを暗号化する。なお、暗号化選択装置１０３における暗号化処理の具体的な手順については、後に詳細に説明する。

【００４０】エージェント送出手段１０５は、暗号化装置１０４において暗号化された暗号化データを含む送信対象のモバイルエージェント３００を、受信側システム２００に送信する。具体的には、エージェント送出手段１０５は、暗号化データを含むモバイルエージェント３００のデータをトランスポータ３１０の中に配置し、受信側システム２００のエージェント受信手段２０１に対してＪａｖａのｖｉｓｉｔの因数として引き渡す。その結果、Ｊａｖａは訪問先へのストリームを開き、トランスポータオブジェクトを直列化してストリームに入力す

る。なおこの時、エージェント送出手段１０５は、モバイルエージェント３００のクラスの定義も受信側システム２００に送信する。

【００４１】受信側システム２００は、送信側システム１００より送信されるモバイルエージェント３００を受信し、モバイルエージェント３００に含まれる暗号化データを復号化して所望の処理を行う装置であって、送信側システム１００と同じく例えばパーソナルコンピュータ等の計算機装置である。受信側システム２００は、エージェント受信手段２０１、復号化装置２０３及びエージェントプレース２０２を有する。

【００４２】エージェント受信手段２０１は、Ｊａｖａの機能としてストリームからモバイルエージェント３００を取り出し、モバイルエージェントオブジェクトの実体をエージェントプレース２０２上に復元する。また、送信側システム１００からは、モバイルエージェント３００とともにモバイルエージェント３００のクラス定義データが転送されるので、エージェント受信手段２０１は、クラスローダによって新たなクラスをＪａｖａＶｉｒｔｕａｌマシンに登録する。これにより、モバイルエージェント３００の新たなタイマが動作を始める。

【００４３】エージェントプレース２０２は、復元されたモバイルエージェント３００に独自のスレッドを割り当てることにより、モバイルエージェント３００を起動する。

【００４４】復号化装置２０３は、復元されたモバイルエージェントに含まれる暗号化データを復号化し、復号化されたデータをモバイルエージェント３００に供する。なお、復号化装置２０３における復号化処理の具体的な手順については、後に詳細に説明する。

【００４５】保持するデータが復号化されたモバイルエージェント３００は、１つの独立したオブジェクトとして、その内部に記述されているプログラムによって、そのモバイルエージェント３００に固有の所望の処理を行う。その固有の処理が終了したら、次に、モバイルエージェント３００は、その所望の処理の結果及びモバイルエージェント３００自身を操作する処理を行う。この処理は、モバイルエージェント３００の動作としてモバイルエージェント３００中に記述してあるプログラムに従って実行される場合と、エージェントプレース２０２が独自に処理を選択し実行する場合とがある。しかしどちらの場合も、その処理としては、複製、消滅又は帰着のいずれかのの処理が実行されることとなる。

【００４６】複製は、モバイルエージェント３００自身の複製（クローン）を生成し、そのクローンエージェントをさらなる別の訪問先へ、図示せぬ受信側システム２００より訪問させる処理である。これは、例えば、最初に訪れたエージェントが単なるハブで他のエージェントプレースへのポインタに過ぎない場合等に、エージェントプレース２０２の判断により選択され実行される。つまり、訪れたエージェントプレースは、他のエージェントプレースへの案内場所であり、かつ、その案内場所が複数ある場合に、エージェントプレースはエージェントを次に訪れるエージェントプレースの場所の数だけ複製（クローン）し、それぞれのエージェントプレースに移動させる。なお、この複製処理が行われた場合、複製される前の元のモバイルエージェント３００は、最終的に消滅する。従って、この時点でエージェントが保持していたデータへのアクセスは不可能になる。

【００４７】消滅は、エージェントの寿命（最初に設定された有効期間）が訪れた場合に、自身のスレッドを停止し、エージェントプレース２０２からメモリを開放する処理である。メモリの実質的な開放は、Ｊａｖａのガベージコレクションによって行われる。モバイルエージェント３００は、送信側システム１００の暗号化選択装置１０３によって最適な暗号化強度のアルゴリズム及び鍵長が選択されて暗号化が行われているので、寿命が訪れるまでにアタックされるどのような鍵無し復号化も、モバイルエージェント３００の消滅までに復号化は行えない。

【００４８】帰着は、最初の指示によってホームである送信側システム１００に戻る処理である。これは、訪問先でモバイルエージェント３００が得た処理結果を送信側システム１００に持ち帰るような場合に相当する。その場合は、受信側システム２００内の図示しないエージェント送信手段によってモバイルエージェント３００は送信側システム１００に送信され、送信側システム１００の図示しないエージェント受信手段によりモバイルエージェント３００は受信される。送信側システム１００に戻ったモバイルエージェント３００は、持ち帰った処理結果をエージェントプレース１０１に返した後、消滅の処理を行う。つまり、スレッドを停止し、ホームのＪａｖａのガベージコレクターによりメモリを開放する。この時点でホームに戻ったエージェントが保持していたデータへのアクセスも不可能になる。

【００４９】次に、このような構成のデータ処理システム１の送信側システム１００の暗号化選択装置１０３及び暗号化装置１０４、及び、受信側システム２００の復号化装置２０３における暗号化及び復号化の具体的処理について、図２及び図３を参照して説明する。

【００５０】まず、送信側システム１００の暗号化選択装置１０３における、暗号化強度の選択条件、選択方法について、図２を参照して説明する。図２は、暗号化されたモバイルエージェント３００を復号鍵を知らずに復号化する時間と、モバイルエージェント３００の寿命の関係を示す図である。時間Ｔａを暗号化アルゴリズムＡで暗号化されたデータを復号鍵ａを用いて復号化するのに要する時間、時間Ｔｂをその暗号化データを復号鍵を知らずに復号化するのに要する時間とすると、一般にＴａ＜Ｔｂの関係が成り立つ。そして、時間Ｔをモバイル

エージェントの寿命とすると、Ｔａ＜Ｔ＜Ｔｂの関係が成り立つ場合に、この暗号化アルゴリズム及び鍵の選択は適切である、すなわち暗号化システムとして成立すると言える。すなわち、正当な復号鍵ａを保持する者は暗号化データを復号して平文データを獲得することができ、復号鍵を知らずに暗号化データの復号を試みた場合には、復号化を達成する前にモバイルエージェント自体が寿命により消滅してしまう状態である。

【００５１】ところで、この条件は、復号鍵を知らずに復号化する時間Ｔｂとモバイルエージェント３００の寿命Ｔとの関係で示すと、図２の斜線領域で示す条件となり、この斜線領域に含まれる条件であれば、どのような条件であっても暗号化システムとしての目的、性能は達成されたものとなる。従って、暗号化システムの効率を考えた場合には、図２に領域３２１で示すような、復号鍵を知らずに復号化が行える時間Ｔｂがモバイルエージェントの寿命Ｔよりもやや長くなる程度の暗号化強度が好ましい、すなわち暗号化アルゴリズム及び鍵長が、安全にデータを送信するために必要かつ十分な最適な条件と言える。逆に言えば、図２に領域３２２で示すような、復号化鍵を知らずに復号するのに要する時間Ｔｂがモバイルエージェントの寿命Ａよりも遥かに長いようなアルゴリズム又は鍵長は、復号化が達成される遥か前にモバイルエージェント自体が消滅しているため無意味であり、そのような暗号化を行うこと自体が計算機リソースを無駄使いしていると言える。

【００５２】従って、送信側システム１００の暗号化選択装置１０３においては、エージェントブレース１０１で設定されたモバイルエージェント３００の寿命Ｔに基づいて、復号鍵を知らずに復号化が行える時間Ｔｂがモバイルエージェントの寿命Ｔよりもやや長くなるような、図２に領域３２１で示すような最適な暗号化強度、すなわちアルゴリズム及び鍵長を動的に選択し、モバイルエージェント３００に適用する。

【００５３】次に、送信側システム１００の暗号化装置１０４及び受信側システム２００の復号化装置２０３における実際の暗号化及び復号化の手順について、図３を参照して説明する。インターネット等のネットワークを介して不特定多数との暗号通信のためには、通常、秘密鍵方式の暗号化手法を用いるが、本実施の形態のようにモバイルエージェント３００を用いて秘密鍵方式の暗号化通信を行うには、基本的に以下のような手順で処理を行う。

（１）送信前に送信先のエージェントブレースの公開鍵を入手する。

（２）公開鍵でデータを暗号化する。

（３）送信先のエージェントブレースに移動する。

（４）送信先のエージェントブレースは秘密鍵でエージェントが保持するデータを復号化する。

【００５４】以下、この手順による暗号化及び復号化の

具体的な手順について、図３に示すフローチャートを参照して説明する。まず、送信側システム１００の暗号化装置１０４においては、暗号化対象のデータ４０１からＭＤ５一方向ハッシュ関数４０２等によって、メッセージダイジェスト４０３を作成する（ステップＳ１１）。次に、ＲＳＡ秘密鍵４０４等によって、ステップＳ１１で作成したメッセージダイジェスト４０３を暗号化する（ステップＳ１２）。一方、乱数４０６を鍵として、ＤＥＳ等の共有鍵暗号化形式の共有鍵４０７を生成する（ステップＳ１３）。

【００５５】そして、ステップＳ１３で生成した共有暗号鍵４０７によって、ステップＳ１２で生成した暗号化メッセージダイジェスト４０５及びデータ４０１を暗号化し、暗号化データ４０８を生成する（ステップＳ１４）。また、訪問先の公開鍵４０９によって、ステップＳ１３で生成した共有鍵を暗号化し、暗号化された共有鍵４１０を生成する（ステップＳ１５）。そして、ステップＳ１４で生成した暗号化データ４０８及びステップＳ１５で生成した暗号化共有鍵４１０を、受信側システム２００に送信する（ステップＳ１６）。

【００５６】受信側システム２００の復号化装置２０３においては、送信され暗号化データ４０８及び暗号化共有鍵４１０を受信し（ステップＳ１６）、秘密鍵４１１によって送信されてきた暗号化共有鍵４１０を復号化して共有鍵４０７を取り出す（ステップＳ１７）。そして、送られてきた暗号化データ４０８を、ステップＳ１７で復号化した共有鍵４０７で復号化することにより、復号化された平文のデータ４０１が得られる（ステップＳ１８）。

【００５７】ステップＳ１８の復号化の際には、暗号化メッセージダイジェスト４０５も同時に得られるので、これを、送信側システム１００側の公開鍵４１３で復号化し、送信側システム１００側で生成されたメッセージダイジェスト４０３を得る（ステップＳ１９）。また、ステップＳ１８で復号化したデータ４０１から、ＭＤ５一方向ハッシュ４０２によってメッセージダイジェスト４１４を作成する（ステップＳ２０）。そして、ステップＳ１９で復号化したメッセージダイジェスト４０３と、ステップＳ２０で新たに作成したメッセージダイジェスト４１４を比較する（ステップＳ２１）。その結果、これらのメッセージダイジェスト４０３．４１４が一致した場合は、送信側の認証と改竄がないことが証明され、データ４０１の授受が完了する。

【００５８】最後に、このような構成のデータ処理システム１の動作について、モバイルエージェント３００の動作として、図４を参照してまとめて説明する。まず、送信側システム１００において、エージェントの親プログラムであるエージェントブレース１０１が、送信側システム１００の計算機リソース上のメモリにエージェントの実体（オブジェクト）を確保することにより、モバ

イルエージェント３００の実体が生成される（ステップＳ３１）。このときに、エージェントプレース２０１は、モバイルエージェント３００に、消滅するまでの有効期限（寿命）をセットする。生成されたモバイルエージェント３００は、エージェントプレース１０１へ登録されることにより配置され（ステップＳ３２）、モバイルエージェント３００に固有のスレッドを起動することにより起動される（ステップＳ３３）。

【００５９】何らかの入力項目がある場合には、モバイルエージェント３００はここで入力フェーズに入り、エージェント入出力装置１０２を介した入力操作を受け付ける（ステップＳ３４）。次に、エージェントのサイズと寿命によって、暗号化選択装置１０３を介して最適な暗号化アルゴリズム及び鍵長を検索し、暗号化装置１０４よって保持するデータを暗号化する（ステップＳ３５）。そして、エージェント送出手段１０５より、受信側システム２００（訪問先）へ送信される（ステップＳ３６）。

【００６０】受信側システム２００においては、エージェント受信手段２０８がＪａｖａの機能としてストリームからエージェントを取り出し、エージェントオブジェクトの実体をエージェントプレース２０３上に復元し（ステップＳ３７）、同時に転送されるエージェントのクラスをクラスローダＪａｖａＶｉｒｔｕａｌマシンに登録することにより、新たにエージェント２０３の寿命タイマが動作する。そして、モバイルエージェント３００は、再び再び独自のスレッドを開始し起動する（ステップＳ３８）。

【００６１】起動されたら、モバイルエージェント３００は、復号化装置２０３を介して暗号化データを復号化し（ステップＳ３９）、復号化されたデータを用いてエージェント固有の処理を行う（ステップＳ４０）。そして、エージェント固有の処理が終了したら、その処理結果及び自らのその後の処理として、モバイルエージェント３００内部に記載されているプログラムに従って、又はエージェントプレース２０２からの制御に基づいて、複製（ステップＳ４１）、消滅（ステップＳ４２）、帰着（ステップＳ４３）のいずれかの処理を実行する。

【００６２】このように、本実施の形態のデータ処理システム１によれば、モバイルエージェント３００が自律的に保持しているデータを管理する方法として、モバイルエージェント３００自体に有効期限を設けるようにした。モバイルエージェントの送信者が、ネットワーク上にモバイルエージェント３００を送出した後は、モバイルエージェント３００が移動やクローン化を自律的に行うために、送信者は、今現在どこに自分の送り出したモバイルエージェント３００が存在しているかもわからないし、通信手段もわからないのが一般的である。しかし、モバイルエージェントに寿命を設定することによって、送信者から制御されなくとも、モバイルエージェントは生成されてから一定期間経つと、そのデータともども自動的に寿命を迎えて消滅する。そして、消滅すればデータも失われ、盗聴や不正アクセス等の危険はなくなる。従って、このような自律型のモバイルエージェント３００を用いた自律型のプログラムオブジェクトを用いたデータ処理システムにおいても、適切なセキュリティが確保される。

【００６３】なお、場合によっては、まだ使命を終えてないにも関わらず寿命を迎えてしまうモバイルエージェントも存在することになるが、モバイルエージェントをベースとしたアプリケーションは、場合によっては応えが帰らない場合もあるというベストエフォート型のサービスとして認識されることにより障害はなくなる。

【００６４】なお、本実施の形態は、本発明の理解を容易にするために記載されたものであって本発明を何ら限定するものではない。本実施の形態に開示された各要素は、本発明の技術的範囲に属する全ての設計変更や均等物をも含み、また、任意好適な種々の改変が可能である。例えば、本実施の形態においては、自律型のプログラムオブジェクトとして、いわゆるモバイルエージェントを示したが、本発明においては、汎用的な計算機装置やノード装置等で構成される一般的なプラットフォーム、環境中において、装置に依存した特定の制御動作に依存することなく自律的に動作可能なオブジェクトであれば、任意のオブジェクトでよく、何ら本実施の形態のオブジェクトの具体的な構成、動作手順等に限定されるものではない。

【００６５】また、本実施の形態においては、送信側システム１００及び受信側システム２００は、汎用的なネットワークに各々１つのノードとして配置されている装置であるとしたが、２台の例えばパーソナルコンピュータ等が直接に通信回線で接続されたような処理システムや、よりローカルな通信ネットワークにより接続された各端末装置等であってもよく、何らシステムゼンタの構成が限定されるものではない。その他、暗号化及び復号化の方法等も任意の方法でよい。

【図面の簡単な説明】

【図１】図１は、本発明の一実施の形態のデータ処理システムの構成を示すブロック図である。

【図２】図２は、暗号化されたモバイルエージェントを復号鍵を知らずに復号化する時間とモバイルエージェントの寿命の関係を示す図である。

【図３】図３は、図１に示したデータ処理システムにおける、送信側システムの暗号化装置及び受信側システムの復号化装置における暗号化及び復号化の手順を示すフローチャートである。

【図４】図４は、図１に示したデータ処理システムにおけるモバイルエージェントの動作を示すフローチャートである。

【符号の説明】

21

１００…送信側システム
１０１…エージェントプレース
１０２…エージェント入出力装置
１０３…暗号化選択装置
１０４…暗号化装置
１０５…エージェント送出手段
２００…受信側システム
２０１…エージェント受信手段
２０２…エージェントプレース
２０３…復号化装置
３００…モバイルエージェント
４０１…データ

【図１】

22

＊４０２…ＭＤ５一方向ハッシュ関数
４０３…メッセージダイジェスト
４０４…送信側秘密鍵（ＲＳＡ秘密鍵）
４０５…暗号化メッセージダイジェスト
４０６…乱数
４０７…共有暗号鍵
４０８…暗号化データ
４０９…受信側公開鍵
４１０…暗号化共有鍵
４１１…受信側秘密鍵
４１３…送信側公開鍵
＊　４１４…メッセージダイジェスト

【図２】

図 1

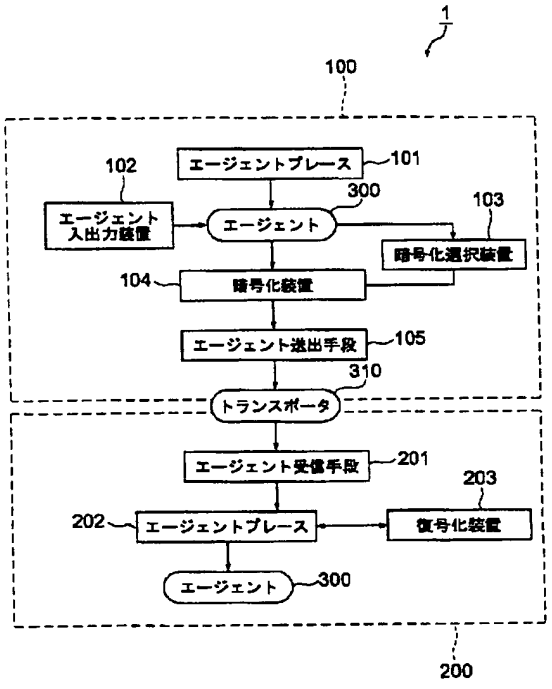
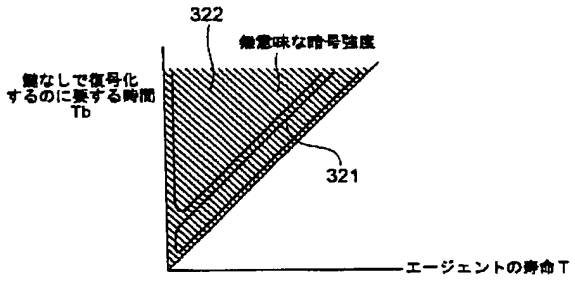
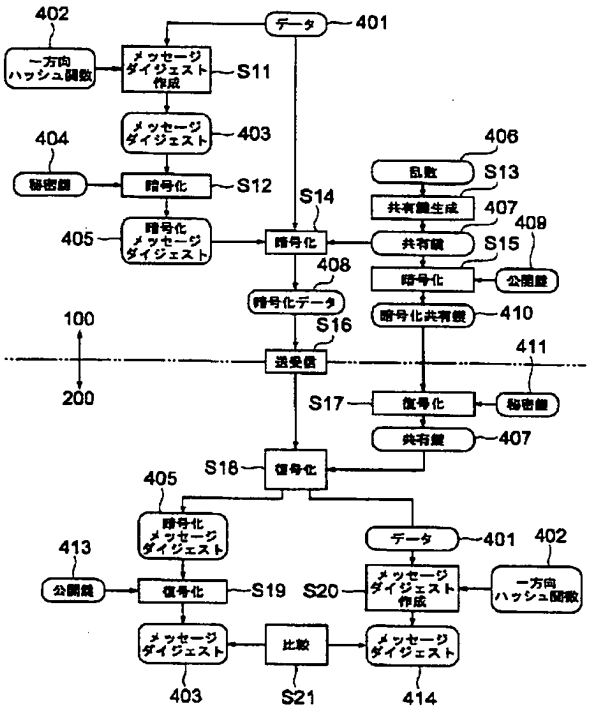


図 2



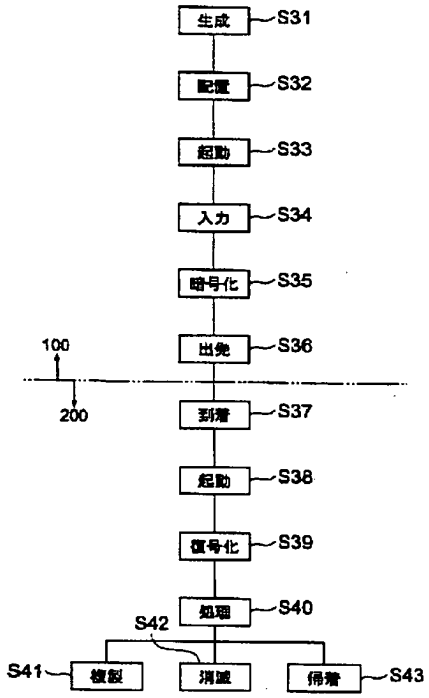
【図３】

図 3


402
データ
401
一方向ハッシュ関数
メッセージダイジェスト作成
S11
メッセージダイジェスト
403
404
秘密鍵
暗号化
S12
406
乱数
S13
共有鍵生成
407
S14
405
暗号化メッセージダイジェスト
暗号化
共有鍵
S15
409
公開鍵
408
暗号化データ
暗号化共有鍵
410
100
S16
送受信
411
200
S17
復号化
秘密鍵
共有鍵
407
S18
復号化
405
暗号化メッセージダイジェスト
データ
401
402
413
公開鍵
復号化
S19
S20
メッセージダイジェスト作成
一方向ハッシュ関数
メッセージダイジェスト
比較
メッセージダイジェスト
403
S21
414

【図４】

図 4


生成
S31
配置
S32
起動
S33
入力
S34
暗号化
S35
100
出発
S36
200
到着
S37
起動
S38
復号化
S39
処理
S40
S42
S41
複製
消滅
帰着
S43